

UNITED STATES DISTRICT COURT
 for the
 Southern District of Ohio

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 2007 GRAY KIA RONDO, VIN# KNAFG526477111654; and }
 A T-MOBILE CELLULAR PHONE ASSIGNED NUMBER }
 (614) 615-5569 }
 (614) 615-5569 }

Case No. *J. D. my. 11-EPD*

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
 See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):
 See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

The application is based on these facts:

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Tyler Schwab
 Applicant's signature

Special Agent Tyler Schwab
 Printed name and title



Elizabeth Preston Deavers
 Judge's signature
 Elizabeth Preston Deavers, U.S. Magistrate Judge
 Printed name and title

Sworn to before me and signed in my presence *via Facetime*

Date: *March 8, 2021*
 City and state: *Columbus, OH*

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:
2007 GRAY KIA RONDO, VIN#
KNAFG526477111654; and

A T-MOBILE CELLULAR PHONE
ASSIGNED NUMBER (614) 615-5569

Case No. D:21-mj-1602

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE

I, Tyler Schwab, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search a 2007 gray Kia Rondo, VIN# KNAFG526477111654, hereinafter the "VEHICLE," and a T-Mobile cellular phone assigned number (614) 615-5569, hereinafter the "PHONE," both described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since January 6, 2019. Your Affiant has been assigned to the FBI Joint Terrorism Task Force ("JTTF"). During my current assignment at the JTTF, I have been a Case Agent and Co-Case Agent for multiple international and domestic terrorism investigations. While assigned to the JTTF, your Affiant has received specialized training in international terrorism. Furthermore, I have received training in computer-related crimes as well as in the criminal use of email, social media, and telephonic communications.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds); and 40 U.S.C. §§ 5104(e)(2) (violent entry, disorderly conduct, and other offenses on Capitol grounds) (the “Target Offenses”), that have been committed by JARED ADAMS (“the Subject”) and other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, the Subject, as well as others observed by the Subject. There is also probable cause to search the VEHICLE and PHONE, further described in Attachment A, for the things described in Attachment B.

PROBABLE CAUSE

Background – The U.S. Capitol on January 6, 2021

5. USCP, the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906 on January 6, 2021.

6. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to

south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and off limits to the public on January 6, 2021.

7. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

8. On January 6, 2021, the exterior plaza of the U.S. Capitol was closed to members of the public.

9. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020 ("Certification"). The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

10. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the U.S. Capitol building, and USCP were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

11. At around 1:00 p.m. EST, known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

12. At around 1:30 p.m. EST, USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building in part because of a suspicious package found nearby. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

13. Media reporting showed a group of individuals outside of the Capitol chanting, "Hang Mike Pence." I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

14. At approximately 2:00 p.m., some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons

checks by U.S. Capitol Police Officers or other authorized security officials. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

15. Shortly after 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows an unknown individual saying to a crowd outside the Capitol building, “We’re gonna fucking take this,” which your affiant believes was a reference to “taking” the U.S. Capitol.



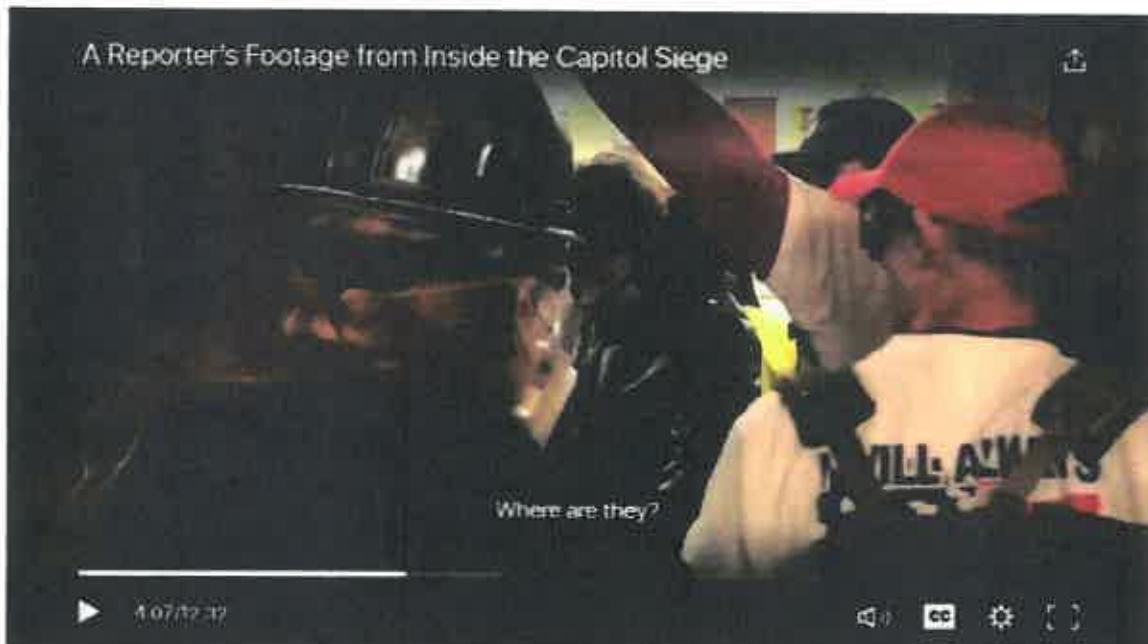
16. Shortly thereafter, at approximately 2:20 p.m. members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. That is, at or about this time, USCP ordered all nearby staff, Senators, and reporters into the Senate chamber and locked it down. USCP ordered a similar lockdown in the House chamber. As the subjects attempted to break into the House chamber, by breaking the windows on the chamber door, law enforcement were forced to draw their weapons to protect the victims sheltering inside.

17. At approximately 2:30 p.m. EST, known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the U.S. Capitol on both the west side and the east side of the building. Once inside, the subjects broke windows and doors, destroyed property, stole property, and assaulted federal police officers. Many of the federal police officers were injured and several were admitted to the hospital. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and Tasers. They also took police equipment from overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine. These actions by the unknown individuals resulted in the disruption and ultimate delay of the vote Certification.

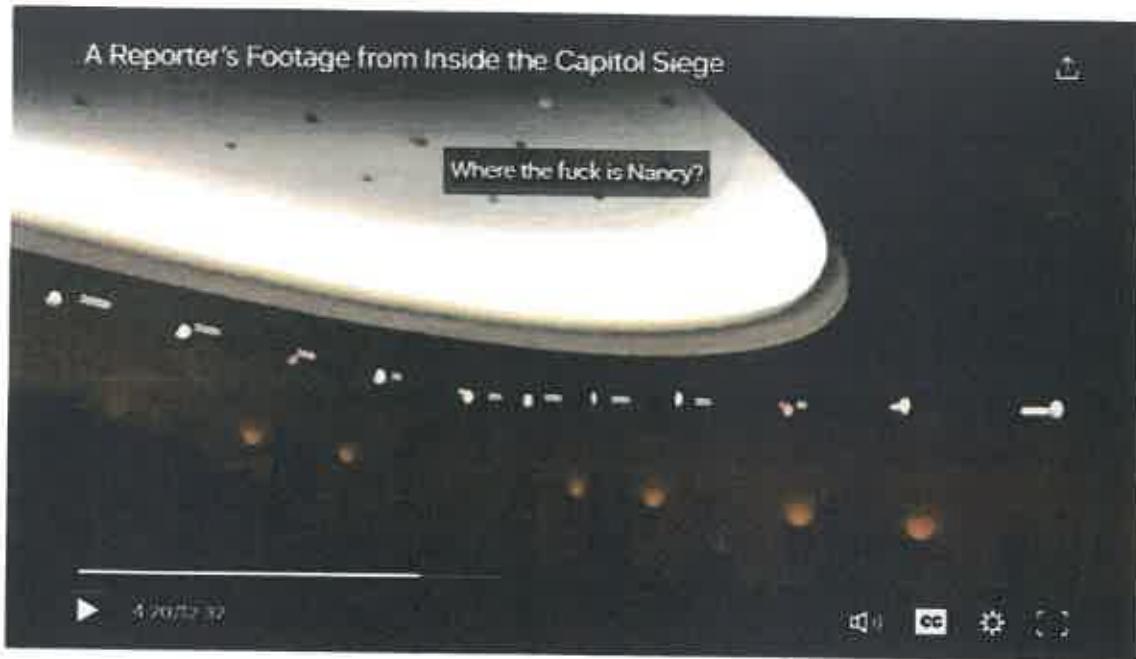
18. Also at approximately 2:30 p.m. EST, USCP ordered the evacuation of lawmakers, Vice President Mike Pence, and president pro tempore of the Senate, Charles Grassley, for their safety.

19. At around 2:45 p.m. EST, subjects broke into the office of House Speaker Nancy Pelosi.

20. At around 2:47 p.m., subjects broke into the United States Senate Chamber. Publicly available video shows an individual asking, “Where are they?” as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word “they” refers to members of Congress.



21. After subjects forced entry into the Senate Chamber, publicly available video shows that an individual asked, “Where the fuck is Nancy?” Based upon other comments and the context, law enforcement believes that the “Nancy” being referenced was the Speaker of the House of Representatives, Nancy Pelosi.



22. An unknown subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated "A Matter of Time Justice is Coming."



23. During the time when the subjects were inside the Capitol building, multiple subjects were observed inside the US Capitol wearing what appears to be, based upon my training and experience, tactical vests and carrying flex cuffs. Based upon my knowledge, training, and experience, I know that flex cuffs are a manner of restraint that are designed to be carried in situations where a large number of individuals were expected to be taken into custody.





24. At around 2:48 p.m. EST, DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m.

25. At around 2:45 p.m. EST, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

26. At about 3:25 p.m. EST, law enforcement officers cleared the Senate floor.

27. Between 3:25 and around 6:30 p.m. EST, law enforcement was able to clear the U.S. Capitol of all of the subjects.

28. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the

dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

29. Beginning around 8:00 p.m., the Senate resumed work on the Certification.
30. Beginning around 9:00 p.m., the House resumed work on the Certification.
31. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3 a.m. on January 7, 2021.
32. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.
33. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate

with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

34. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging and stealing property. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

35. Photos below, available on various publicly available news, social media, and other media show some of the subjects within the U.S. Capitol during the riot. In several of these photos, the individuals who broke into the U.S. Capitol can be seen holding and using cell phones, including to take pictures and/or videos:



¹ <https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/>



² <https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1>.



Facts Specific to This Application

36. On approximately January 7, 2021, an informant (W-1), provided a tip to the FBI identifying ADAMS. W-1 identified himself. He did not know ADAMS personally, but explained that he was friends with a high school classmate of ADAMS'. W-1 provided the information regarding ADAMS voluntarily, without financial compensation or other enticement/inducement, and W-1's information was corroborated through a review of publicly available information and law enforcement records. W-1 told the FBI that ADAMS is associated with the Instagram account with a username of *jokerschild1994* and had videotaped himself breaking into the U.S. Capitol.

³<https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e>

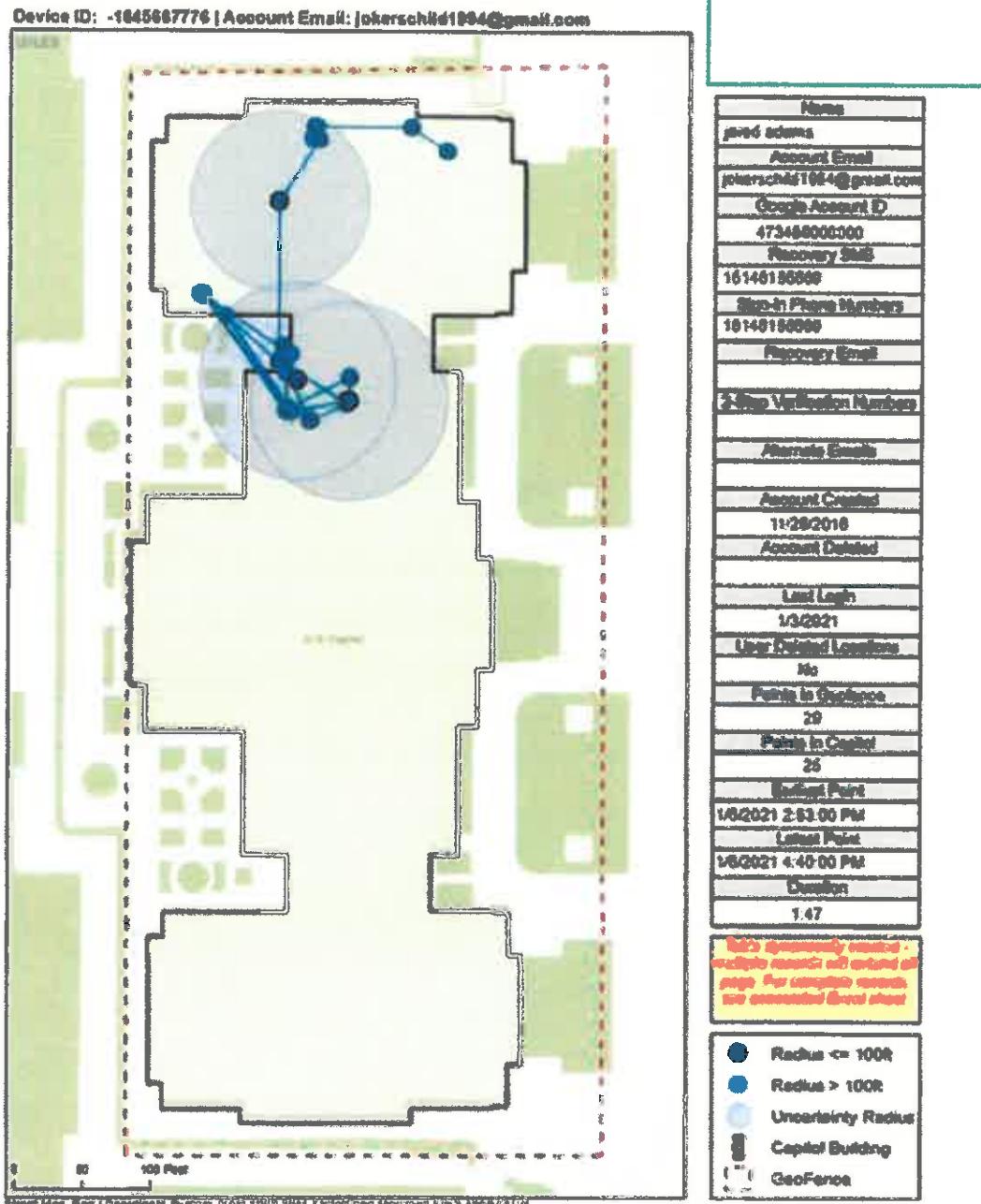
37. W-2 provided a screen recording of ADAMS' Instagram story (video) which was posted on January 7, 2021. The FBI reviewed the Instagram story, which includes close-up video of individuals breaking into the Capitol, photos of Washington, D.C., landmarks, and statements including "We stormed the Capitol building and the senate today! I can tell my grandchildren I was there!" It also includes video of a crowd walking toward the Capitol, and someone (who seems to be the recorder of the video) can be heard saying, in substance, that they were going to break into the Capitol and that the Capitol police better have enough pepper spray.

38. Instagram records confirmed that the Instagram account jokerschild1994 is associated with ADAMS, with an e-mail address of jokerschild1994@gmail.com, and T-Mobile phone number 614-615-5569 (the number associated with the PHONE). Records provided by Facebook (username jared.adams.35325) include the same e-mail address and phone number. Records lawfully provided by Google reveal that the mobile device associated with jokerschild1994@gmail.com belonged to a Google account registered in the name of Jared Hunter ADAMS. The Google account also lists a recovery SMS phone number that matches the PHONE, the same number as identified above. Information from law enforcement databases indicates that ADAMS lives in Plain City, Ohio. The FBI reviewed ADAMS' application for an Ohio driver's license, which contains the same phone number associated with the PHONE. In addition, three managers of apartment complexes where ADAMS either lived or applied for an apartment between 2017 and July 2019 also confirmed his same phone number, associated with the PHONE.

39. According to records lawfully obtained from Google, a mobile device associated with jokerschild1994@gmail.com was present at the U.S. Capitol on January 6, 2021. Google estimates device location using sources including GPS data and information about nearby Wi-Fi access points and Bluetooth beacons. This location data varies in its accuracy, depending on the source(s) of the data. As a result, Google assigns a “maps display radius” for each location data point. Thus, where Google estimates that its location data is accurate to within 10 meters, Google assigns a “maps display radius” of 10 meters to the location data point. Finally, Google reports that its “maps display radius” reflects the actual location of the covered device approximately 68% of the time. In this case, Google location data shows that a device associated with jokerschild1994@gmail.com was within the U.S. Capitol from approximately 2:53 p.m. until approximately 4:40 p.m. for a total approximate time inside the U.S. Capitol of one hour and 47 minutes. Google records show that the “maps display radius” for this location data was less than 100 feet, which encompasses an area that is partially within the U.S. Capitol Building.

40. As illustrated in the map below, the listed locations encompass areas that are partially within the U.S. Capitol Building during 2:53 p.m. until 4:40 p.m. Specifically, Google location data shows that a device associated with jokerschild1994@gmail.com, with the sign-in phone number associated with the PHONE, was within the U.S. Capitol at the times and locations shown in the map below (at the locations reflected by each darker blue circle), with the “maps display radius” reflected in the map below (as reflected in a lighter blue ring around each darker blue circle). In addition, as illustrated in the map below, the listed locations were entirely within

areas of the U.S. Capitol Grounds which were restricted on January 6, 2021.



41. The FBI has reviewed the available information for jokerschild1994@gmail.com in order to determine whether there was any evidence that devices associated with that address could have lawfully been inside the U.S. Capitol Building on January 6, 2021. The information for that address did not match any information for persons lawfully within the Capitol. Accordingly, I believe that the individual possessing this device was not authorized to be within the U.S. Capitol Building on January 6, 2021.

42. According to records obtained through a search warrant which was served on AT&T, on January 6, 2021, in and around the time of the incident, the PHONE was identified as having utilized a cell site consistent with providing service to a geographic area that includes the interior of the United States Capitol building.

43. Your Affiant located JARED ADAMS on U.S. Capitol Police security video filmed inside the U.S. Capitol. Photos from this video footage were created. In the footage, ADAMS is wearing a gray Ohio State hooded sweatshirt and a backwards blue/gray baseball cap. Your affiant compared ADAMS' driver's license photo to photographs below and reasonably believes that the individual circled is ADAMS.



44. On February 19, 2021, the FBI interviewed JARED ADAMS' former roommate (W-2). W-2 lived with ADAMS for approximately two years, between 2017 and 2019. During the

interview, W-2 identified ADAMS in the photos that were created from the video footage from inside the U.S. Capitol. W-2 viewed two photos. When W-2 viewed the photo below, he circled, drew an arrow toward, and initialed near a person he thought was ADAMS. W-2 was not confident that the person he circled, drew an arrow to, and initialed was JARED ADAMS. The person W-2 identified is not the same person identified by the FBI, and does not appear to be ADAMS.



45. W-2 was then shown the photo below. W-2 circled, drew an arrow toward, and initialed an individual he stated he was positive was ADAMS. The individual whom W-2 identified was the same individual the FBI had identified as ADAMS.



46. The FBI has conducted the following investigation associating the VEHICLE to ADAMS:

- a. A law enforcement database check for JAREDADAMS, date of birth June 21, 1994, social security number xxx-xx-0008, returned a 2007 Gray Kia Rondo with VIN# KNAFG526477111654 registered to JARED ADAMS (reference attachment A for photographs).
- b. On February 19, 2021, ADAMS' former roommate, W3, informed the FBI that JAREDADAMS may be living out of his vehicle at a truck wash.

- c. On February 19, 2021, ADAMS was observed sleeping in the backseat of a Gray Kia Rondo with OH license plate HUS1516 (the VEHICLE), registered to ADAMS. The VEHICLE was parked in the parking lot of Professional Truck Washing Services located at 4255 Roberts Road, Columbus, Ohio 43228.
- d. On February 20, 2021, ADAMS was observed sitting in a Gray Kia Rondo with OH license plate HUS1516, registered to ADAMS. The VEHICLE was parked in the parking lot of Professional Truck Washing Services located at 4255 Roberts Road, Columbus, Ohio 43228.
- e. On February 24, 2021, ADAMS was observed laying down in the driver's seat in a Gray Kia Rondo with OH license plate HUS1516, registered to ADAMS. The VEHICLE was parked in the parking lot of Professional Truck Washing Services located at 4255 Roberts Road, Columbus, Ohio 43228.
- f. On February 25, 2021, ADAMS was observed sitting in the front driver seat and then crawling into the backseat and laying down in a Gray Kia Rondo with OH license plate HUS1516, registered to ADAMS. The VEHICLE was parked in the parking lot of Professional Truck Washing Services located at 4255 Roberts Road, Columbus, Ohio 43228.

47. There is evidence that ADAMS had in his possession a digital device while at the U.S. Capitol on January 6, 2021, and that he is the user of the PHONE, including the following:

- a. On January 7, 2021, the user of the Instagram account associated with ADAMS posted on Instagram images from the Capitol riot outside the U.S. Capitol Building.
- b. On approximately January 7, 2021, W-1 informed the FBI that JARED ADAMS posted videos of himself breaking into the Capitol.
- c. W-2 provided a screen recording of JARED ADAMS' Instagram story which was posted on January 7, 2021. The FBI reviewed the Instagram story, which included the statement "We stormed the Capitol building and the senate today! I can tell my grandchildren I was there!"
- d. Google records show that a device associated with ADAMS' Google account (jokerschild1994@gmail.com) and the number associated with the PHONE was within the U.S. Capitol on January 6, 2021.
- e. In addition to Google records, Instagram records and ADAMS' Ohio driver's license identify the number associated with the PHONE, and three managers of apartment complexes where identified ADAMS' phone number as the number of the PHONE.

f. AT&T records identified the PHONE as having utilized a cell site consistent with providing service to a geographic area that includes the interior of the United States Capitol building on January 6, 2021.

48. In addition, based on photos and videos of the offenses that date, numerous persons committing the Target Offenses possessed digital devices that they used to record and post photos and videos of themselves and others committing those offenses. Further, based on the investigation, numerous persons committing the Target Offenses possessed digital devices to communicate with other individuals to plan their attendance at the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

49. Moreover, it is well known that virtually all adults in the United States use mobile digital devices. In a fact sheet from June 12, 2019, the Pew Research Center for Internet & Technology estimated that 96% of Americans owned at least one cellular phone, and that that same 2019 report estimated that 81% of Americans use at least one smartphone. See Mobile Fact Sheet, <https://www.pewresearch.org/internet/fact-sheet/mobile> (last visited January 9, 2021). Based on my training and experience, I also know that individuals typically carry their mobile digital devices with them at almost all times, including typically keeping them at home when they are at home, with them on their person or in their vehicles when traveling by motor vehicle. This is especially the case with mobile digital devices that are capable of storing large amounts of data and that serve

as an individual's primary means of communication. In ADAMS' case, the evidence ADAMS took his cellular telephone with him when traveling to Washington, D.C., and while in the U.S. Capitol Building, confirms that ADAMS keeps his cellular telephone with him.

50. I also know from my training and experience, and from conversations with other law enforcement officers, that items such as the clothing that ADAMS appears to be wearing in the photos from the riot are often stored or left in vehicles, particularly where an individual is sleeping in his or her vehicle, rather than in a residence, as ADAMS recently has. Further, I know that evidence of travel is often stored or discarded in vehicles, such as toll receipts, maps, map notations, written or printed directions, receipts for food or lodging, or other evidence of destinations, routes, and travel contacts.

51. In addition, in my training and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and Apple iCloud service. Thus, there is reason to believe that evidence of the offense that originally resided on the Subject's cell phone may also be saved to other devices within the VEHICLE. Moreover, here, as widely reported in the news media related to this matter, many individuals committing the Target Offenses kept and posted videos, photos, and commentary about their participation in these offenses, essentially bragging about their participation. Based on that, there is also probable cause to believe that evidence related to these offenses may have been

transferred to and stored on digital devices beyond the particular digital device the Subject possessed during the offense.

52. Based on my training and experience, and on conversations I have had with other law enforcement officers, I know that some individuals who participate in activities aimed at disrupting or interfering with governmental and/or law enforcement operations have been known to use anonymizing services and/or applications capable of encrypting communications so the content of these conversations is on the electronic device that had been used to send or receive the communications.

53. The property to be searched includes any laptop computers, mobile phones and/or tablets owned, used, or controlled by JARED ADAMS, including but not limited to the PHONE.

54. Your affiant further submits that there is probable cause to believe that the VEHICLE and property found therein, including laptop computers, mobile phones, and/or tablets owned, used, or controlled by the Subject, and the PHONE, contain evidence, fruits, contraband, instrumentalities, and information of the criminal violations because the Subject may have recorded or otherwise obtained evidence of other persons crimes while on the Capitol Grounds and inside of the Capitol Building on January 6, 2021.

TECHNICAL TERMS

55. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See 18 U.S.C. § 1030(e)(1).* Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic,

or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global

positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

c. A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touchscreen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The “Internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. “Internet Service Providers,” or “ISPs,” are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line (“DSL”), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a username or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A “modem” translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A “router” often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire

or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet.

In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

- i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.
- ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.
- o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by

establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network—hence the name “virtual private network.” The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. “Encryption” is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. “Malware,” short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

56. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found in the VEHICLE or on the PHONE, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices (including, but not limited to, the PHONE). Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including the criminal offenses referenced above, use digital devices, like the Device(s), to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Device(s), documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other “Short Message Service” (“SMS”) messages; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts. Similarly, your affiant has seen examples of suspects communicating after a crime via text message (or other online chat functions) to discuss where incriminating items have been hidden, where and what police are doing to investigate the crime, and whether any witnesses have implicated them. Many different people worked together to breach the Capitol on January 6, and concerted actions among some participants may involve discussion and planning, which is regularly done by online chats or texts.

b. Based on my training and experience, I know that people who engage in the foregoing criminal activity often use their cell phones in ways that reveal their location and/or activities in preparation for and while engaging in criminal activity. This may include location information (e.g.,

GPS data), application usage information (e.g., Internet search inquiries), and images or video recordings relevant to the criminal activity. For example, law enforcement may see videos or photographs on a suspect's phone taken at or near key points in the crime. Such video and images often include identifying landmarks, buildings, or backgrounds that help place the suspect in an important location related to the crime, and may have data associated with them allowing law enforcement to identify the location where the photograph or video was taken. Other phones record the directions and GPS information provided to the phone user when traveling from one location to another. Furthermore, I know from my training and experience that any application enabling communication with others often includes communication that sheds light on the cell phone user's location and activity during a particular time period. Just as people making plans often update each other via text regarding when they will arrive somewhere or where they will meet, suspects often communicate with others regarding where they are going or when they plan on arriving at a location.

c. Based on my training and experience, I know that phones typically list device information (such as the associated IMEI, Phone Number, Android or Apple ID) and linked user accounts. The device information, includes for instance the phone numbers associated with the phone, the IMEI,

and sometimes even includes the name of the phone as provided by the phone user (such as “JohnDoe’s I-phone”). Linked user accounts include account names and handles used to log in to apps regularly used on the phone, such as the account names used on social media sites like Instagram, email accounts used, or online communication platforms, like Textnow and Snapchat. Both device information and linked accounts are key both for identifying the phone user’s location during the crime and for identifying the user of the phone. Based on my training and experience, I know that linked accounts, such as a cell phone number or a related email account, also provide key information to indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, if the phone number associated with the phone is a number frequently used by friends or associates of the suspect to contact him or her, the government’s identification of the phone number will assist in proving who was using the phone at the time key activity on the phone occurred. Similarly, your affiant has regularly seen the suspect’s full name be listed in the email address linked to a phone, which clearly helps identify the user of the phone.

d. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

e. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have

been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

57. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of

how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the

user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device

evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device to document involvement in or incite other to join events such as the Capitol riot, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain

data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

58. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are

being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself.

Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not

discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and

application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alphanumeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate

and retrieve digital information, records, or evidence within the scope of this warrant.

59. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical on-site search of the VEHICLE.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the VEHICLE, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s), including the PHONE), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the site where the VEHICLE is searched. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and

review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to

whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

BIOMETRIC ACCESS TO DEVICE(S)

60. This warrant permits law enforcement agents to obtain from the person of JARED ADAMS (but not any other individuals present at the VEHICLE at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

61. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These

biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

62. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

63. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple’s “Face ID”) have different names but operate similarly to Trusted Face.

64. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature

is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

65. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

66. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

67. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric

features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

68. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s); (2) hold the Device(s) in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

69. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

REQUEST FOR SEALING

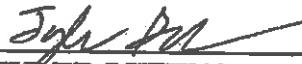
70. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation, and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and

disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation, such as by leading to the destruction of evidence, and may severely jeopardize its effectiveness. Premature disclosure of the content of this affidavit and related documents may also cause the subject of the investigation to destroy evidence before the search warrant can be executed. It could also compromise the ability of the United States to locate and arrest the subject of the investigation.

CONCLUSION

71. I submit that this affidavit supports probable cause for a warrant to search the VEHICLE and PHONE described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,


TYLER SCHWAB
Special Agent
FEDERAL BUREAU OF
INVESTIGATION

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on

ELIZABETH PRESTON DEAVERS 3/8/2021
UNITED STATES MAGISTRATE JUDGE

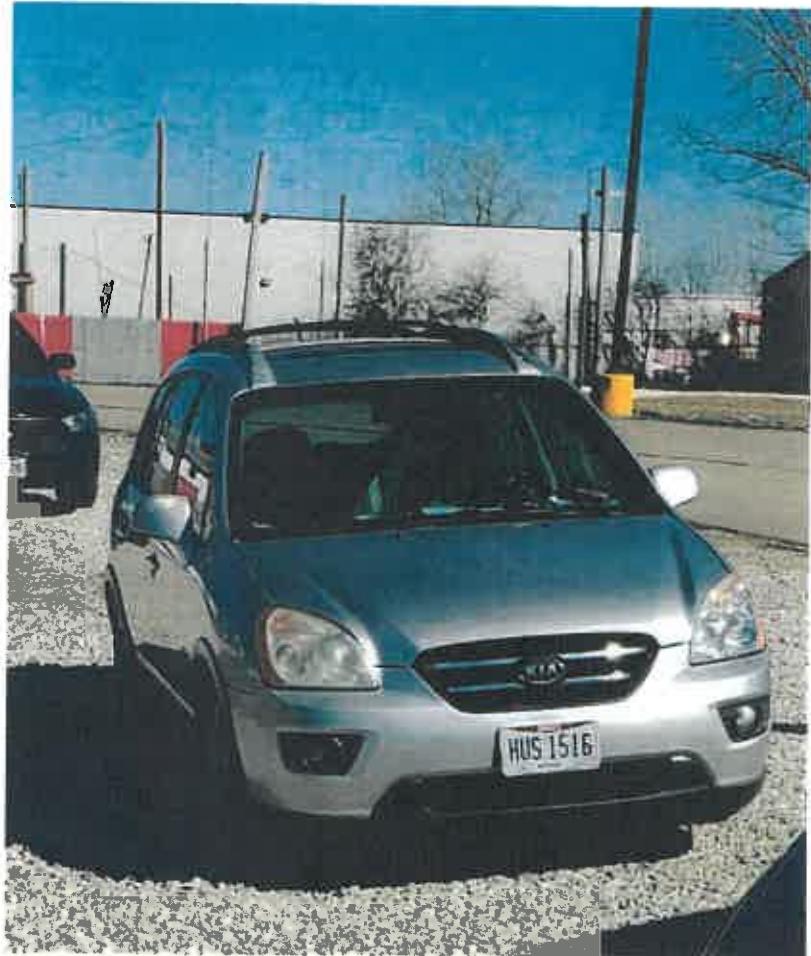
ATTACHMENT A

Property to be searched

The property to be searched is a 2007 Gray Kia Rondo, VIN# KNAFG526477111654, Ohio license plate HUS1516 (the “VEHICLE”) and a T-Mobile cell phone assigned number of (614) 615-5569 (the “PHONE”). Photos of the VEHICLE are below:







ATTACHMENT B

Property to be seized

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. §§ 1752 (a) (1) (knowingly entering or remaining in any restricted building or grounds without lawful authority), 1752(a)(2) (knowingly engaging in disorderly or disruptive conduct in restricted building), and 40 U.S.C. §§ 5104(e)(2)(D) (disorderly or disruptive conduct in the Capitol Buildings), and (G) (parading, demonstrating, or picketing in any of the Capitol Buildings); (the “Target Offenses”) that have been committed by JARED ADAMS (the “Subject”) and other identified and unidentified persons , as described in the search warrant affidavit, including, but not limited to:

- a. Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;
- b. Evidence concerning unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;
- c. Evidence concerning awareness of the official proceeding that was to take place at Congress on January 6, 2021, i.e. the certification process of the 2020 Presidential Election;
- d. Evidence concerning efforts to disrupt the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;

- e. Evidence concerning the breach and unlawful entry of the U.S. Capitol and any conspiracy or plan to do so on January 6, 2021;
- f. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;
- g. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;
- h. Evidence concerning materials, devices, or tools that were used to unlawfully enter the U.S. Capitol by deceit or by force, including weapons and elements used to breach the building or to counter efforts by law-enforcement, such as pepper spray or smoke grenades;
- i. Evidence of communication devices, including closed circuit radios or walkie-talkies, that could have been used by co-conspirators to communicate during the unlawful entry into the U.S. Capitol;
- j. Evidence of the state of mind of the subject and/or other co-conspirators, e.g., intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and
- k. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation, or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

2. Records and information that constitute evidence of identity, including but not limited to:

a. Clothing worn by the subject, to include gray Ohio State hooded sweatshirt and a blue/gray baseball cap.

b. Clothing and other articles that reflect evidence of having participated in unlawful activity at the U.S. Capitol, including evidence of pepper spray or other non-lethal crowd control remnants;

3. Records and information-including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements-relating to:

a. Any records and/or evidence revealing the Subject's presence at the January 6, 2021, riot;

b. Any physical records, such as receipts for travel, which may serve to prove evidence of travel of to or from Washington D.C. from December of 2020 through January of 2021;

c. The Subject's (and other's) motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and

d. The Subject's (and other's) activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021.

4. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above (including but not limited to the PHONE), hereinafter the "Device(s)":

- a. Evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging, logs, photographs, and correspondence;
- b. Evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;
- d. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
- e. Evidence of the times the Device(s) was used;
- f. Passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
- g. Documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
- h. Records of or information about Internet Protocol addresses used by the Device(s);
- i. Records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. Routers, modems, and network equipment used to connect computers to the Internet.

During the execution of the search of the VEHICLE and PHONE described in Attachment A, law enforcement personnel are also specifically authorized to obtain from JARED ADAMS (but not any other individuals present at the VEHICLE at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as finger/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

- (a) Any of the Device(s) found in the VEHICLE,
- (b) Where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the

aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if Agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which Device(s), the Agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "digital devices" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems,

routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.